SECUREPURDUE NEWS
www.purdue.edu/securepurdue

December, 2011
Volume 6, Issue 4

All the news that's secure to print.

FROM the CISO

By Scott Ksander
Executive Director
IT Networks & Security

The end of the year is a good time to review the past and look forward to the future. (It is also a good time to make a backup of your critical data and change the batteries in your smoke detectors). Network access continues to grow and integrate itself into everything around us. Over two billion people now have broadband Internet access and it is predicted that in the next ten years, five billion people will own a smartphone, giving them access to the Internet from nearly anywhere.

It is already clear this holiday shopping season that the "smartphone" is changing how we shop. It allows us to do research for prices and features real time, even inside the store. Consumer review sites provide evaluation of devices or products, and shopping sites allow you to quickly compare prices at different retailers. It is a comparison shopper's dream come true.

Some of you may receive or gift yourself a new technology gadget this Christmas: Kindle Fire, iPad2, Droid phone, iPhone, or whatever. All these devices have wireless capabilities. A new wireless router might also be a good choice to allow use of those devices while sitting next to the fireplace. Why should you upgrade your current, working router? Speed and security. Your older router may not be able to stream movies or play games as fast as the newer models. Older routers didn't always default to good security settings. Be sure to check out the article on page 3 to learn more about properly setting up your wireless router.

With expanded functionality comes increased opportunities for abuse. Mobile devices are going to continue to be the "great opportunity" for bad guys to exploit. Good security tools for mobile devices are just starting to become available. This is an area where I believe we will see some major improvements in 2012. We will continue to keep you informed as we learn of new advances in this area. In the meantime, be aware that data on your mobile device will continue to be a prime target. Be sure that you know what data is on your mobile device and that you take steps to secure it.

This will be my last column for the SecurePurdue newsletter. I will be joining the ranks of official Purdue retirees in January. Over the last 25 years I have seen great accomplishments in IT at Purdue, and it has been my honor and pleasure to work with and for each of you.

In the last 5 years, and through the SecurePurdue initiative, Purdue has made major improvements in our view of IT security. I thank you for your support of those improvements. We are not "done," however, and even greater challenges are ahead. I know that Purdue can count on your continued support of and attention to IT security matters.

So, for one final time, remember to always be careful out there.

In this issue

Cyber Season: Tips for Safe Online Shopping

The holiday shopping season has already begun. To reduce the risk of spam, viruses and accidental downloading of malware that can infiltrate your personal data, use these steps to protect yourself.

1. Use your desktop PC or laptop, not your mobile device, to shop. Your desktop browser is likely to be more secure than your mobile device or apps.

2. If using your mobile device to purchase items, protect sensitive information, like credit card numbers, by password-protecting both your mobile device and its memory card.

3. Make sure you update your anti-virus and anti-malware programs continually.

4. Treat social networking sites with the same caution as other web sites. Social sites are a growing target for fraud.

5. Be cautious of special offers. If it looks too good to be true, it probably is. Notice if you are receiving more spam and double your diligence to prevent being a victim.

Online Shopping Scam - Use of Social Engineering

The number of spam emails in my inbox has increased lately. I would guess as a result of the forthcoming cyber shopping season. Because of the economy and loss in investments, many people are shopping for bargains. So what good fortune when an email pops in your inbox that offers you that special gift you want to buy for your family member but now at a price you can afford!! Tip number 5 from online shopping warns against deals too good to be true but... you have an office mate that always gets bargains and nothing bad happens. So how do you know what to look for? Here are some tips to keep your online shopping safe and give you the savings you are looking for.

1. Don't use the link in the email which could take you to an exact copy of the legitimate site. Go directly to the website where you would purchase your item. Whether that is Amazon, Apple, or something else, type the address in the browser to go there. If you go to the fake site and place your order, you have given away your credit card information. You also won't ever see the product you thought you were purchasing!! Now you have no gift to give and will deal with credit card fraud charges on your account.

3. If the deal looks really good, then test them out. Set up an account with as little information as possible or fake information. See what the email response looks like. Scammers just don't realize that terrible grammer and poor spelling tip cautious customers to leave their site fast. This is the first red flag.

4. Look at the URL listed in the email response. Is it exactly the same as the real establishment or really close to the legitimate site? This may be a red flag that they may not be who they pretend to be.

5. When you move through their site to purchase an item, does the URL have HTTPS? This ensures you that your transaction is secure. Red flag #3 if it isn't.

If it isn't adding up, you will be ahead to pay the full price of the item. You will receive the product and your credit card will be intact from attempts of fraud. You can relax, drink some eggnog or other holiday beverage and know you are secure.

Computerworld Magazine Describes New Malware Threat

A freelance computer consultant in California built virtually undetectable malware. He used various tricks to get people to install this on their computers. His malware allowed a very personal invasion of their privacy. He read their e-mails, watched them through webcams and listened to them through the microphones on their computers. The information he obtained from his lurking in their computer allowed him to play psychological games with his victims.

The method of distributing his malware was often done by disguising a song on peer-to-peer networks or e-mail, posting it in an instant message to victims disguised as a video.

He is accused of "sextortion" - a new threat where hackers break into your computer and search for compromising photographs that they threaten to post unless some deal is struck.

For a link to the entire article:
http://www.computerworld.com/s/article/9219701/

SPOTLIGHT

Wireless Router Set Up

You were good and Santa brought lots of wonderful devices that use a wireless environment. Your old router may not be up to the task of running video or games on your iPad. Now might be the time to buy a new wireless router. Our family operates devices on two floors and the 6 antennae router is adequate to our task. We have 3 laptops and one printer routinely accessing the router. No one has complained of dropped Internet connections. Do a little online research to find what will fit your needs.

The newer routers support the Wi-Fi Protected Access (WPA) protocol which replaced the very weak Wired Equivalent Privacy (WEP). You want the WPA2 protocal router. The latest wireless router technology standard is 802.11n (also called Wireless-N). Wireless-N is faster that Wireless-G and has a wider range so that you can maintain a high data rate flow throughout your home.

Another feature of new routers is the ability to have a "guest" network so friends can still access their devices. An easy to remember password can be given to your friends but your network runs separate from the guess account.

Before you sit down to read on your Kindle Fire or browse the Internet on your new iPad 2, take a few minutes to configure your new high speed wireless router. Here are some of the things to do that will protect your wireless network:

1. Secure your wireless router or access point - set a password as administrator and store this in a password vault or create an easy to remember password so you will remember it. Check out our 2012 Password tips aricle for more information. If you forget the password you will have to reset it to the default settings, losing any configuration changes you may have made.

2. Enable the Wi-Fi Protected Access (WPA) or better yet, WPA2 which is also referred to as WPA-AES This encryption provides much better protection than Wired Equivalency Privacy (WEP). If your router doesn't have this option, it is time to purchase a new router.

3. Reduce the transmitter power so that it transmits inside your home or business but doesn't bleed out too far for others to see.

4. Disable remote administration. Luckily this is usually turned off by default but it doesn't hurt to check this. If you need to use this to resolve an IP address issue, you can turn it back on.

5. You can disable SSID broadcasting to hide your network from neighbors or passers-by as a means to secure your wireless network. Don't let this give you a false sense of security though because a determined hacker with the right software can find it.

Now you can curl up and read your e-book!!

2012 Password Tips

In this day of increased concerns over data and computer security, using "strong passwords" is a must. "Strong passwords" are passwords that are difficult to break but easy for a user to remember.

Longer is Stronger. Use a password with at least 8 characters, including numbers, and upper and lower case letters. This can help bolster the strength of your password. Substituting numbers for letters is a common way to create stronger, yet still memorable passwords. The password "Security" could become "S1c2r3ty" with number's substituting for the vowels.

To create a strong password, include at least one of each of the following:
• A letter• A number• A punctuation mark or control character (e.g., ^s, Ctrl-s)
• include special characters such as @#$%^&*-.

Use a verse where the password is formed from the characters in the verse. For example:"*pybii2012*" is derived from the phrase "Protect your Boiler identity in 2012." This phrase is easily remembered by its creator, but would be very difficult for others to guess.

For more password tips go to: http://www.purdue.edu/securepurdue/bestPractices/passTips.cfm

Plan Your SANS Training for 2012

For those of you wanting training that SANS provides, they will be offering their OnDemand series of training at deep discounts from July 1 -31, 2012.

OnDemand courses give you a span of time to complete the training online by yourself. This is a web-based training that offers a diverse series of courses. A typical four to six day course content, offered in the OnDemand module can cost $4,175, and will be offered for $1000. That is a $3,175 discount. Courses that span 1 - 3 days will cost $500. This is about a 50% discount.

The "window" for registering for OnDemand Training and Voucher Credits is proposed to be July 1-31.
+ SANS Long Courses = $1,000 (4-6 day classes)
+ SANS Short Courses = $500 (1-3 day classes)
+ Minimum order size per transaction: $3,000

For Voucher Credits, the proposed parameters are:
+ SANS "Universal Credits" type
+ Minimum order size per transaction: $5,000

The current NetWars offering (aggregate buy window closes Dec 15) is an excellent training medium also. http://www.ren-isac.net/programs/nw2012/

More information will be available as we get closer to the July 1 date but this gives you time to plan your training needs and save a lot of money.

To read more about SANS online training and assessments, go to:
http://www.sans.org/ondemand/

contact Cherry Delaney for more information:
cdelaney@purdue.edu, 61288.

Joanna Grama appointed to Homeland Security committee on privacy

Joanna Grama, information security policy and compliance director for Purdue University, has been appointed to the Department of Homeland Security's Data Privacy and Integrity Advisory Committee. The committee advises the Department of Homeland Security on how to deal with personally identifiable information, as well as data integrity and other privacy-related matters.

Grama is a member of ITaP's Networks and Security, the American Bar Association's Section of Science and Technology Law, Information Security Committee, as well as a member of the Indiana Bar Association.

Google+

Google+ was released this past summer. It allows you to conduct searches, view advertising, watch YouTube, and view Chrome and Google Maps. Google continues to make acquisitions that have them branching into mobility (Android and Google TV), social media ranking, loyalty programs (Google Wallet), online shopping and deals (Google Offers), retail social reviews (Google Places) and travel services (Google Flight).

Google+ includes new security/privacy featuress allowing users to create cirlcles of networks and determine what information to share and whom to share it with. You can share posts with only certain circles to minimize sending information that might not interest or pertain to them. This allows you greater control over your privacy. Take some time to review the security and privacy features to fit your needs.

SECURITY RESOURCES

- Computerworld Website Article
http://blogs.computerworld.com/security/cybercrime_hacking

- SANS OnDemand Training
http://www.sans.org/ondemand/

- *REN-ISAC NetWars offfer*
http://www.ren-isac.net/programs/nw2012/

- SecurePurdue Website
http://www.purdue.edu/securepurdue/bestPractices/passTips.cfm
- Computer World
http://www.computerworld.com/s/article/9219701/